

Treball de Fi de Grau

Estudi empíric sobre el minat de criptomonedes des de la web

Tecnologies de la informació

Mohamed Chait

Director

Pere Barlet Ros

Arquitectura de Computadors

27 de Maig de 2019

Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

Resum

Les pàgines utilitzen els anuncis publicitaris com a mètode de monetització per permetre als usuaris accedir de manera gratuïta al seus continguts. Degut a això els usuaris han començat a evitar els anuncis mitjançant bloquejadors d'anuncis provocant un menor benefici econòmic a les pàgines. L'increment del valor de les criptomonedes en els últims anys ha creat una alternativa al mètode tradicional de monetització. La mineria de criptomonedes és el conjunt de processos necessaris per validar i processar les transaccions en la cadena de blocs. Aquests processos requereixen recursos computacionals elevats que poden ser paral·lelitzables i distribuïts en una pàgina web perquè els usuaris facin aquesta feina sense prèvia notificació o avís mitjançant codi Javascript que es descarregat en entrar a la pàgina.

En aquest projecte es fa un estudi en profunditat del minat de criptomonedes per crear una eina de detecció de minat de criptomonedes automatitzat. S'ha utilitzat l'eina creada per analitzar les 100.000 pàgines més visitades segons el rànquing d'Alexa. S'han trobat 56 pàgines minant criptomonedes. Finalment, es comparen els resultats amb la extensió més popular de detecció NoCoin del navegador Chrome que utilitza un mètode de detecció poc efectiu.

Abstract

Pages use advertising as a monetization method to allow users to access their contents for free. Because of this, users have begun to avoid ads through ad blockers causing lower economic benefits to the pages. The increase in the value of cryptocurrencies in recent years has created an alternative to the traditional method of monetization. The cryptocurrencies mining is the set of processes necessary to validate and process the transactions in the block chain. These processes require high computational resources that can be parallelized and distributed on a webpage so users can do this without prior notice

In this project, an in-depth study of the cryptocurrencies mining is done to create an automated cryptocurrencies mining detection tool. The tool created is used to analyze the 100,000 most visited pages according to the Alexa ranking. 56 pages found mining cryptocurrencies. Finally, the results are compared with the most popular NoCoin detection extension from Chrome Browser that uses an ineffective methodology.

Índex

1. CONTEXT	8
1.1 INTRODUCCIÓ.....	8
1.2 ACTORS IMPLICATS	9
2. ESTAT DE L'ART	9
2.1 HISTÒRIA.....	9
2.2 ESTUDIS ANTERIORS.....	11
2.3 EINES	12
2.4 CONCLUSIÓ.....	12
3.FORMULACIÓ DEL PROBLEMA	13
3.1 OBJECTIUS.....	13
4. DEFINICIÓ DE L'ABAST.....	14
4.1 ABAST	14
4.2 POSSIBLES OBSTACLES	14
5.METODOLOGIA I RIGOR	15
5.1 MÈTODE DE VALIDACIÓ	15
6. PLANIFICACIÓ TEMPORAL	15
6.1 TASQUES.....	16
6.2 DESCRIPCIÓ DE LES TASQUES	17
6.2.1 Planificació del projecte	17
6.2.2 Recerca.....	17
6.2.3 Creació d'un model heurístic.....	17
6.2.4 Desenvolupament software	17
6.2.5 Mesurament.....	17
6.2.6 Documentació	17
6.3 DIAGRAMA DE GANTT INICIAL.....	18
7. RECURSOS.....	19
7.1 RECURSOS HUMANS	19
7.2 RECURSOS HARDWARE	19
7.3 RECURSOS SOFTWARE	19
8. VALORACIÓ D'ALTERNATIVES I PLA D'ACCIÓ.....	20
9. DESVIACIÓ DE LA PLANIFICACIÓ.....	20
9. AUTOAVALUACIÓ DE LA COMPETÈNCIA DE SOSTENIBILITAT	21
10.GESTIÓ ECONÒMICA	21
10.1 COSTOS DE RECURSOS HUMANS	21
10.2 COSTOS DE RECURSOS MATERIALS	22
10.3 COSTOS INDIRECTES.....	23
10.4 CONTINGÈNCIA.....	24
10.5 IMPREVISTOS	24
10.6 PRESSUPOST FINAL	25
10.7 CONTROL DE GESTIÓ	25

11. SOSTENIBILITAT I COMPROMÍS SOCIAL	26
11.1 DIMENSIÓ ECONÒMICA	26
<i>PPP</i>	26
<i>Vida útil</i>	26
<i>Riscos</i>	27
11.2 DIMENSIÓ AMBIENTAL	27
<i>PPP</i>	27
<i>Vida útil</i>	28
<i>Riscos</i>	28
11.3 DIMENSIÓ SOCIAL	28
<i>PPP</i>	28
<i>Vida útil</i>	29
<i>Riscos</i>	29
11.4 MATRIU DE SOSTENIBILITAT	29
12. ANÀLISIS DEL CRYPTOJACKING.....	30
12.1 HTTPS	30
12.2 CODI FONT	31
<i>Monero</i>	31
<i>JSecoin</i>	31
12.3 TIPUS D'EXECUCIONS	32
12.4 DETECCIÓ	32
<i>WebSocket</i>	32
<i>WebAssembly</i>	33
<i>WebWorkers</i>	33
<i>Objecte Window</i>	33
13 DISSENY I IMPLEMENTACIÓ	34
13.1 SERVIDOR SCRAPER	34
13.2 EXTENSIÓ	35
<i>WebSocket</i>	35
<i>WebWorker</i>	35
<i>Objecte Window</i>	36
13.3 SERVIDOR DE REGISTRE	36
13.4 ANALITZADOR	37
SEGURETAT.....	38
CORS	38
CSP	38
PROVES DE VALIDACIÓ	39
REGISTRES.....	39
<i>WebSocket</i>	39
<i>WebWorker</i>	40
<i>Objecte Window</i>	40
RESULTATS.....	42
EXECUCIÓ.....	42
COMPARACIÓ AMB NOCOIN.....	43

IMPACTE DEL CRYPTOJACKING	44
CONSUM ELÈCTRIC	44
BENEFICI	44
INTEGRACIÓ DE CONEIXEMENTS.....	45
CONEIXEMENTS APLICATS	45
ASSOLIMENT DE COMPETÈNCIES	45
CONCLUSIONS.....	46
TREBALL FUTUR	46
AGRAÏMENTS	47
12. BIBLIOGRAFIA	48

Índex de taules

Taula 1.Estimació en hores de les tasques del projecte	16
Taula 2. Diagrama de Gantt	18
Taula 3.Estimació dels costos de recursos humans per rol	22
Taula 4.Estimació dels costos de recursos hardware per producte.....	23
Taula 5.Estimació dels costos indirectes.....	23
Taula 6.Estimació de la contingència.....	24
Taula 7.estimació dels imprevistos	25
Taula 8.estimació del pressupost final	25
Taula 9.Estimació del consum de les activitats del projecte	27
Taula 9.Estimació anual del consum de la vida útil del projecte	28
Taula 10.Valoració de la sostenibilitat.....	29
Taula 11 Base de dades del Domini	36
Taula 12 Base de dades del Registre.....	37
Taula 13 Base de dades del WebSocket.....	37
Taula 14 Base de dades del WebWorker	37

1. Context

1.1 Introducció

Una criptomoneda és una moneda virtual dissenyada per treballar com a medi d'intercanvi utilitzant la criptografia per assegurar les transaccions, controlar la creació de monedes de forma il·legal i per verificar la transferència de les monedes. L'acció de verificar i crear noves monedes s'anomena minar. Totes aquestes funcions provoquen un gran consum computacional per ser realitzades, per això es recompensa als miners amb una quantitat de criptomonedes.

Per minar criptomonedes com Bitcoin o Ethereum es necessiten circuits integrats d'aplicació específica perquè sigui rentable degut al cost d'electricitat. En canvi, altres criptomonedes com Monero es pot minar de manera paral·lelitzable i distribuïda en sistemes de propòsit general com ordinadors o telèfons mòbils. Aquestes últimes es poden introduir en pàgines web mitjançant codi Javascript.

La majoria d'usuaris que naveguen per Internet no saben que els seus dispositius poden ser utilitzats per minar criptomonedes mentre naveguen per les pàgines web. Això afecta negativament en el rendiment i el consum del dispositiu, fins i tot pot arribar a causar danys per sobreescalfament. Un dels objectius d'aquest projecte és conscienciar als usuaris d'aquest nou sistema maliciós.

Aquest projecte que és un treball de fi de grau de l'especialitat de Tecnologies de la Informació de la facultat d'informàtica de la Universitat Politècnica de Barcelona pretén fer un estudi experimental del minar de criptomonedes en les pàgines web més populars segons el rànquing d'Alexa[1].

En aquest projecte es dissenya un programa per detectar de forma dinàmica els scripts¹ de mineria en les pàgines web.

¹ Conjunt d'instruccions informàtiques

1.2 Actors implicats

A continuació es detallarà aquelles persones que afecten o són afectades pel projecte.

Desenvolupador. És l'encarregat de crear les eines per fer l'estudi empíric i aconseguir els objectius dins el termini establert, el desenvolupador que és la mateixa persona que està escrivint la memòria, s'encarregarà també de validar els resultats de l'estudi.

Director del projecte. És el Pere Barlet Ros que tindrà la funció de supervisar i guiar al desenvolupador per tal de satisfer els objectius.

Població. Considerarem la població totes aquelles persones que es beneficiïn dels resultats obtinguts per l'estudi i per les eines que es crearan. Els resultats i les eines poden ser utilitzades per empreses o organitzacions per tal de millorar la seguretat dels navegadors web incloent l'eina en els navegadors. També poden ser emprats per usuaris particulars per identificar les pàgines web que utilitzen el minat de criptomonedes.

2. Estat de l'art

2.1 Història

El minat de criptomonedes des de la web va néixer el 2011 quan es va crear el servei web BitcoinPlus.com que permetia minar criptomonedes *Bitcoin* des de la web mitjançant codi *JavaScript* [2]. Però aquest servei no va ser popular, ja que en aquells temps la dificultat de mineria i el cost del *Bitcoin* eren relativament baixos. A mesura que passaven els anys el valor del *Bitcoin* ha anat augmentat però la complexitat de mineria ha anat creixent fent inviable el minat en les pàgines web d'aquesta moneda.

Però a mitjans d'abril de 2014 es va llençar la criptomoneda *Monero* que facilitava la mineria en dispositius de propòsit general i el seu valor era relativament alt. Això va provocar que a finals de 2017 es crees el servei *Coinhive* que generava una alternativa a la publicitat en les pàgines web permetent incrustar codi *Javascript* de mineria.

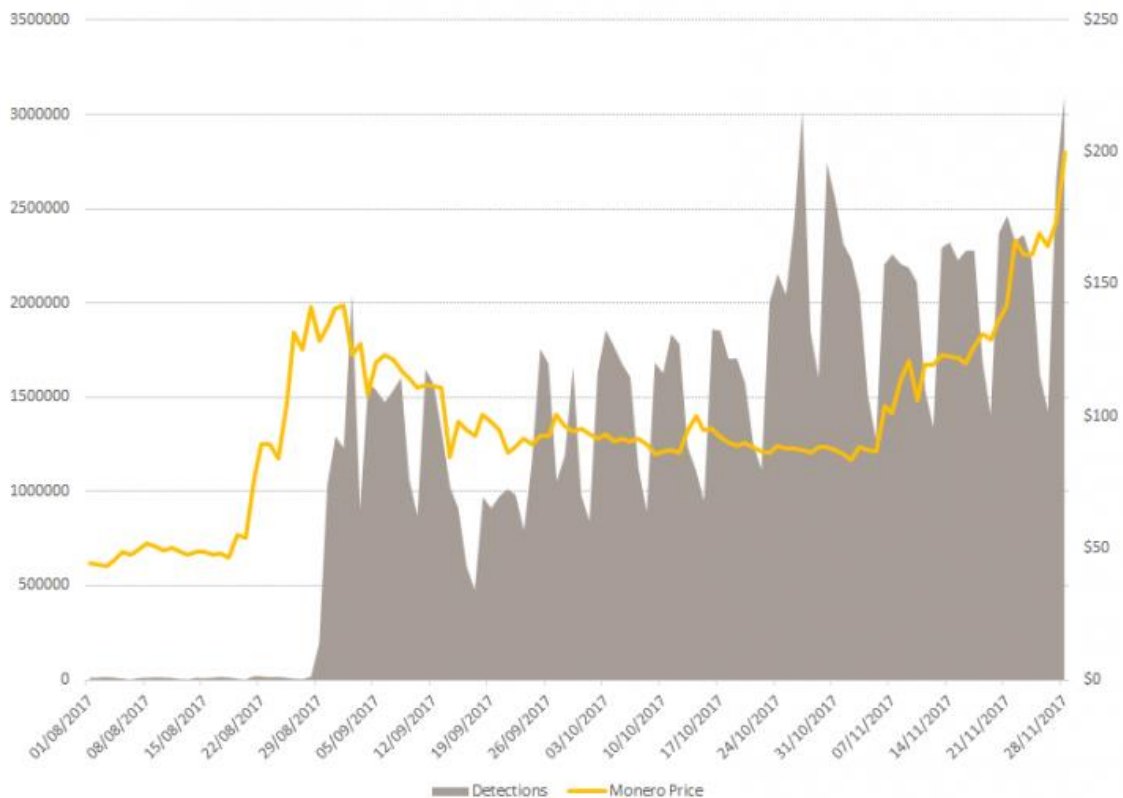


Figura 1 Gràfica mostrant les deteccions de malware de mineria de Symantec i el valor de Monero entre l'agost i desembre de 2017.

Amb la creació d'aquest nou servei va sorgir el *cryptojacking* que és la mineria de criptomonedes no autoritzada per l'usuari. En la figura 1 es mostren les deteccions de *cryptojacking* de l'empresa americana de programari de seguretat informàtica Symantec. S'observa que les deteccions de *cryptojacking* van sorgir amb la creació de Coinhive [3].

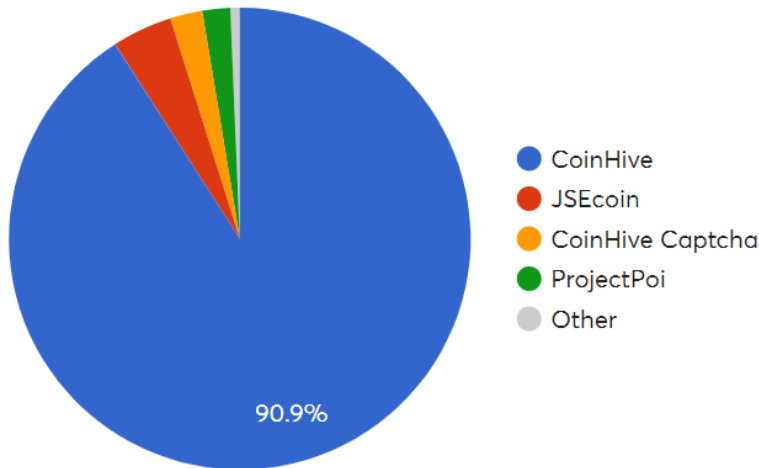
Algunes pàgines web demanen el consentiment de l'usuari per tal de minar utilitzant el codi proporcionat per Coinhive, però segons Malwarebytes [4] només el 1.3% de les pàgines que utilitzen el servei de Coinhive demanen la confirmació per part de l'usuari (Figura 2).

El 8 d Març de 2019, mentre es realitzava aquest projecte, el servei Coinhive ha tancat[5]. El primer factor de la tancada d'aquest servei ha sigut la caiguda del valor de Monero en un 85% durant l'últim any. El segon factor de la tancada és per el *hard fork*²

² És un canvi radical del protocol (algorisme) que provoca la invalidació dels blocs o transaccions anteriors.

de la criptomoneda Monero a principis del 2019, aquest *fork* ha provocat que baixes el *hash rate* més del 50%, es a dir la velocitat de mineria ha sigut reduïda de forma significativa.

Segons el servei Wappalyzer que analitza les tecnologies utilitzades en les pàgines web, el 90,9% de les pàgines web utilitzaven Coinhive[6]. Això afectarà significativament els resultats que s'obtingran amb l'anàlisi de les 50.000 pàgines més populars.



Gràfic 1 Líder del mercat de cryptojacking en les pàgines web segons Wappalyzer

2.2 Estudis anteriors

A l'octubre de 2017 Adguard va realitzar un estudi del minat de criptomonedes en les 100.000 pàgines més populars de la llista d'Alexa [7]. Van trobar 220 pàgines que utilitzaven el minat amb una audiència agregada de 500 milions d'usuaris. Un més després van tornar a fer l'estudi i van observar que el minat de criptomonedes en la web havia crescut un 31% respecte el mes anterior. El 95% del script de minat era de l'empresa *Coinhive*. Amb l'estudi d'1M de pàgines del rànquing d'Alexa és va trobar 1500 pàgines infectades amb els scripts de minat. La metodologia emprada en aquest estudi es desconeguda per tant, serà difícil comparar el nostre estudi amb aquest.

Al desembre de 2017 es va executar un altre estudi (Rauchberger et al. [8]) publicat com a article acadèmic. En aquest estudi és va fer un anàlisi dinàmic del tràfic del WebSocket[9]. Van trobar 3178 pàgines infectades pel minat de criptomonedes en l'anàlisi d'un milió de pàgines del rànquing d'Alexa.

L'últim estudi conegut s'ha fet a l'abril de 2018 per la universitat de Fudan (Hong et al. [10]). La metodologia que es va utilitzar per detectar el minat de criptomonedes és més complexa que els altres estudis.

S'utilitzen dos tipus de detecció, la primera consisteix en detectar quan una pàgina utilitza les llibreries de hashing durant un llarg període que han calculat, ja que aquestes llibreries són necessàries per tal de minar. El segon tipus consisteix en detectar el minat mitjançant la pila d'execució. Observen el comportament de la pila detectant patrons que es repeteixen quan hi ha un script de minat executant-se.

Els resultats obtinguts han sigut favorables, s'han trobat 868 pàgines infectades amb el minat en les 100.000 pàgines més visitades pel rànquing d'Alexa. El nombre de dominis identificats és superior al 260% respecte a l'estudi Adguard.

2.3 Eines

Hi ha eines que permeten protegir als usuaris del *cryptojacking*, una d'aquestes eines és NoCoin que és la més coneguda amb 598.384 usuari[11]. La segona més coneguda és MinerBlock amb 212.081 usuaris [12]. Aquestes eines utilitzen una llista negra per bloquejar scripts coneguts de *cryptojacking*. Malgrat això, en resposta a aquestes eines, els scripts de minat han començat a canviar, ofuscant el codi per evitar ser detectats i utilitzant proxies³.

2.4 Conclusió

Les eines no són eficaces com ja s'ha esmentat anteriorment, per tant no s'utilitzaran per acomplir aquest projecte. Encara que hi haurà una comparació exhaustiva dels resultats amb l'eina més popular NoCoin amb la eina creada en aquest projecte.

³ Servidor intermediari entre el servidor principal i el client

3. Formulació del problema

Amb la creixent popularitat de les criptomonedes en els últims anys han sorgit programes maliciosos per tal de beneficiar-se. Aquests programes utilitzen els recursos dels dispositius per minar mentre s'està en una pàgina web.

Una de les pàgines més conegudes que ha utilitzat el minat per beneficiar-se és la pàgina web de descarrega de torrents *Thepiratebay.org*.

Accedint aquesta pàgina es pot observar amb la figura 3 que l'ús de la CPU es dispara fins al 60% degut al script de minat. En el script s'indica els fils d'execució permesos per executar els scripts de minat (threads:4) i el màxim percentatge d'utilització de la CPU que és d'un 50% (throttle 0.5). També s'indica la criptomoneda que s'està minant, que és Monero (coin: "xmr").

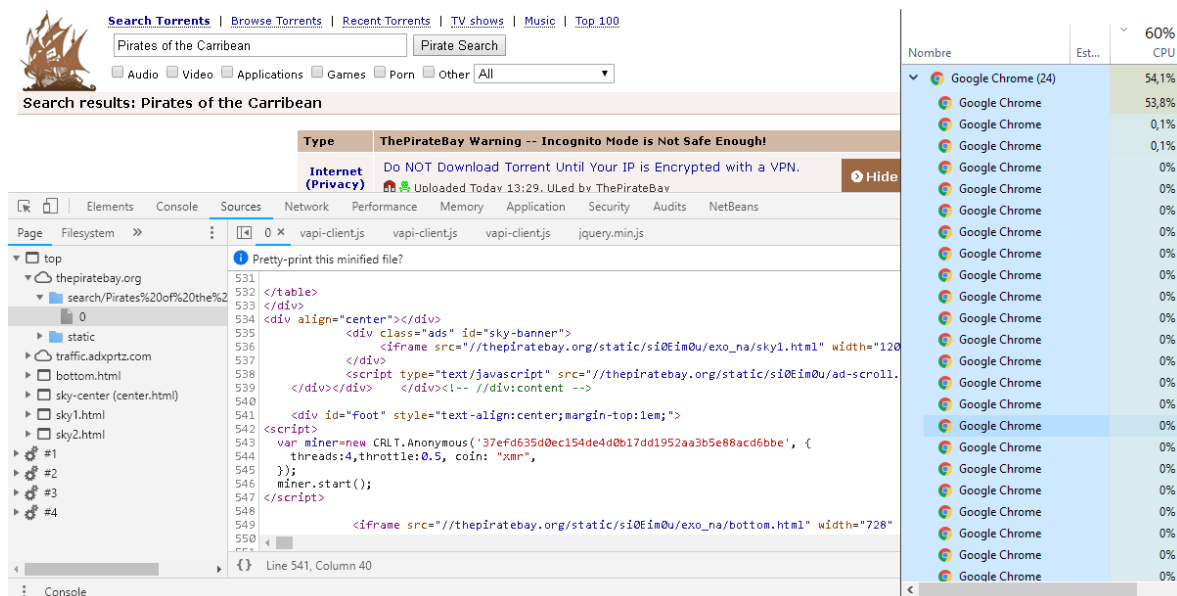


Figura 3. La pàgina web ThePirateBay utilitzant la CPU per minar.

Aquest ús indesitjat dels recursos afecta negativament als usuaris ja que poden causar danys costos i un augment en el consum d'electricitat en els dispositius.

A més a més, les eines existents no són gaire efectives ja que els scripts de minat han anat modificant-se creant noves tècniques per evitar la detecció.

3.1 Objectius

Una vegada explicat el problema que pretén solucionar aquest projecte, podem passar a analitzar els objectius a assolir per tal de satisfer-lo.

4. Definició de l'abast

L'objectiu principal d'aquest projecte es fer un estudi del minat de criptomonedes en les pàgines més populars segons el rànquing d'Alexa.

Per dur a terme l'objectiu principal esmentat anteriorment caldrà efectuar els següents objectius específics :

- 1) Estudi dels scripts actuals de minat de criptomonedes.
- 2) Implementació d'una nova eina per detectar dinàmicament el minat de criptomonedes en les pàgines web.
- 3) Execució de l'eina en les pàgines més visitades respecte el rànquing d'Alexa.
- 4) Anàlisi de resultats.
- 5) Comparativa amb l'extensió NoCoin.

4. Definició de l'abast

4.1 Abast

Per complir l'objectiu principal que és fer l'anàlisi de les pàgines populars, primer caldrà fer un estudi dels diferents tipus de scripts utilitzats actualment pel minat de criptomonedes.

Aquest primer estudi permetrà trobar la millor manera de detectar aquests scripts de forma dinàmica, és a dir, accedint a les pàgines i observant el comportament del codi executat.

Una vegada trobada la millor solució de detecció es començarà a crear una eina de detecció automàtica del minat de criptomonedes.

Finalment s'executarà aquesta eina en les 50.000 pàgines més visitades segons el rànquing d'Alexa.

Per tal de comparar-ho amb NoCoin es crearà una eina per accedir a 50.000 pàgines i registrar les pàgines detectades per l'extensió.

4.2 Possibles obstacles

Com que aquest projecte tracta un tema d'actualitat amb pocs estudis realitzats es poden trobar diferents obstacles.

- 1) Trobar una metodologia de detecció eficaç. Els scripts de minat han anat variant a mesura que han sorgit maneres de contrarestar-los. Això pot provocar que la

metodologia que s'ha utilitzat o s'utilitza en les eines ja existents no siguin eficaços . Per tant s'haurà de crear una metodologia nova i eficaç.

2) Temps limitat. Aquest és una factor rellevant en l'execució d'aquest projecte, per tant s'hauran de plantejar fites a complir per assolir els objectius.

5. Metodologia i rigor

El mètode que s'utilitzarà serà el desenvolupament iteratiu i incremental. Primer es començarà amb els requisits de l'eina de detecció, a continuació es dissenyarà i implantarà. Es començarà amb una eina bàsica per començar la iteració, i s'anirà incrementant les característiques d'aquesta fins a tenir una eina de detecció eficaç sense falsos positius.

En cada iteració caldrà una verificació de l'eina amb un joc de proves per comprovar l'eficàcia de detecció.

5.1 Mètode de validació

Es mantindran reunions de seguiment cada quinze dies amb el director per la validació del treball realitzat de cada iteració realitzada per tal d'afegir noves característiques a l'eina i validar els resultats obtinguts.

A més a més, s'utilitzarà la plataforma web *Slack* que permet la creació de grups privats. Aquesta plataforma s'utilitzarà per fer un grup privat amb el director, el professor Josep Solé i altres estudiants que fan un projecte relacionat amb el *web tracking*. Es compartirà informació relacionada amb el *web tracking*, i es demanarà consell en el transcurs del projecte per aconseguir-lo. A més s'utilitzarà aquesta eina per validar la feina feta amb els companys i els professors.

6. Planificació temporal

Aquest projecte té una duració estimada de 4 mesos, del 18 de febrer fins al 18 de juny. Com que la defensa del treball de Fi de Grau és a principis de juliol es tindrà un parell de setmanes per acabar de refinar el projecte en cas que hi hagi una desviació en la planificació.

El projecte es realitzarà d'una forma seqüencial, ja que només el durà a terme una sola persona. A més a més totes les tasques tenen dependència amb la anterior, per tant només hi ha un camí i és el crític. Per això no cal fer un diagrama de *Pert* ja que l'únic camí que hi ha és el que ens donarà el cost mínim i la duració adequada per fer el projecte.

6.1 Tasques

Tasques	Hores
Planificació del projecte	110
Definició del projecte	20
Gestió del projecte	90
Recerca	40
Detecció de codi Javascript	20
Recerca de scripts de minería	20
Creació d'un model heurístic	50
Rastrear el codi Javascript	25
Detecció de scripts de minat	25
Desenvolupament software	160
Disseny	40
Implementació	80
Verificació de l'eina	20
Mesurament	60
Execució del l'eina en el rànquing	30
Anàlisi de resultats	20
Comparació amb treballs anteriors	10
Documentació	60
Documentació de la memòria	40
Preparació de la presentació oral	20
Total	480

Taula 1. Estimació en hores de les tasques del projecte

6.2 Descripció de les tasques

6.2.1 Planificació del projecte

Aquesta fase servirà per definir i gestionar el projecte que es realitzarà que inclourà l'abast del projecte, la contextualització, la planificació temporal i per últim el pressupost i sostenibilitat.

6.2.2 Recerca

En aquesta fase s'estudiarà com detectar el codi Javascript d'un navegador web. A més a més es cercaran els scripts de mineria existents.

6.2.3 Creació d'un model heurístic

Aquesta fase es farà una vegada trobada la manera més eficaç per detectar el minat de criptomonedes. Primer de tot es buscaran eines per rastrejar el codi javascript d'un navegador web i poder analitzar el codi font de les pàgines web, una vegada es té el codi font s'estudiarà com detectar els scripts de minat.

6.2.4 Desenvolupament software

En aquesta fase es començarà amb el disseny de l'eina que es crearà per la detecció del minat, s'estudiaran les diferents llibreries i eines existents per fer una implementació eficaç, i finalment es finalitzarà verificant l'eina amb un joc de proves.

6.2.5 Mesurament

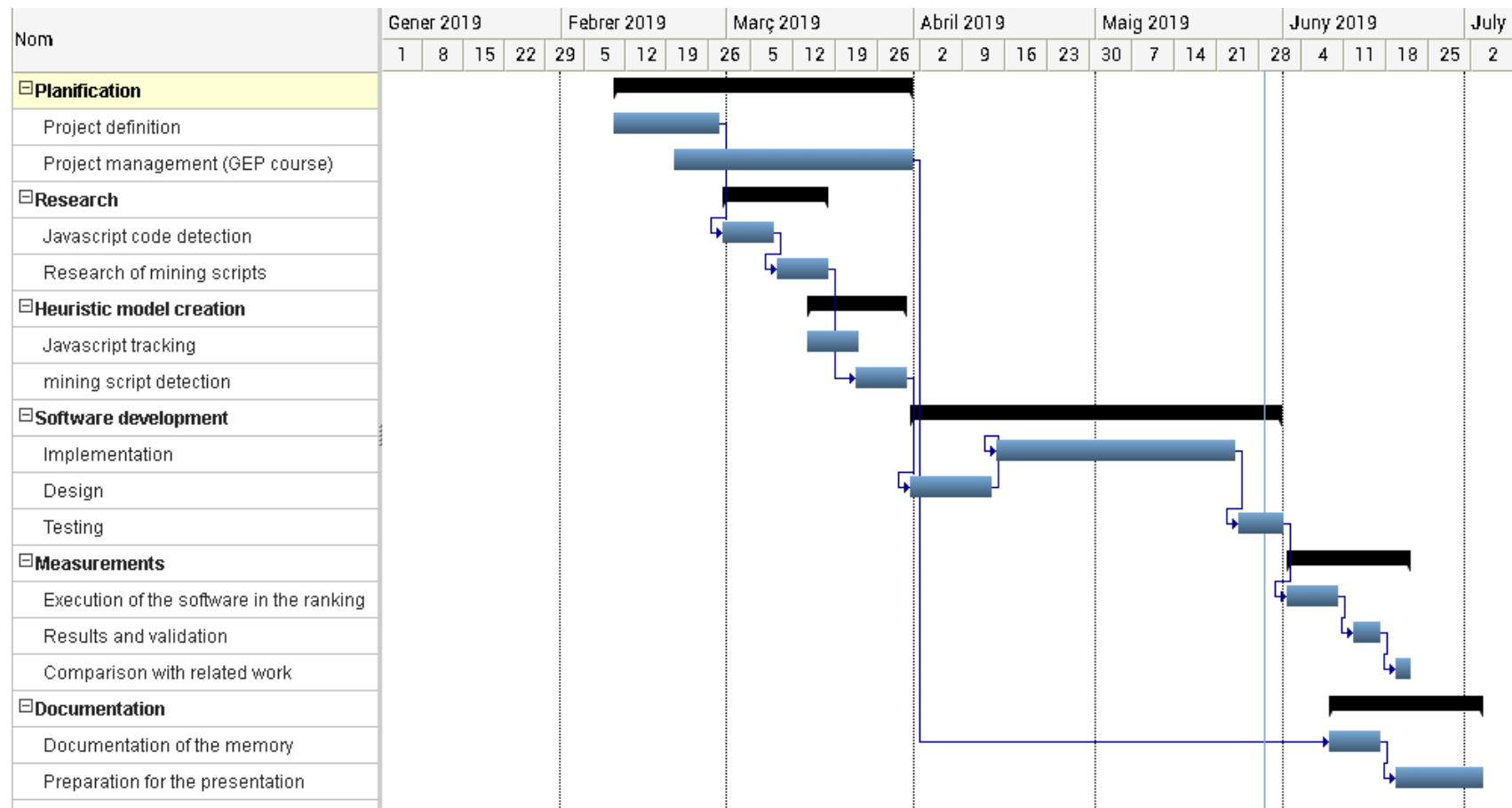
Aquesta fase consistirà en executar l'eina creada en les pàgines web més conegudes segons el rànquing d'Alexa i es farà un anàlisi dels resultats. Finalment es compararan els resultats amb altres estudis.

6.2.6 Documentació

Per últim es documentarà tot el treball realitzat en aquestes fases i es prepararà la defensa oral del projecte.

6.3 Diagrama de Gantt inicial

En el Gantt següent es pot veure les diferents tasques amb les dependències de cada tasca.



Taula 2. Diagrama de Gantt

7. Recursos

Per a realitzar el projecte s'utilitzaran diferents eines, tant software com hardware.

7.1 Recursos humans

Com a recurs humà només es disposarà d'una sola persona per desenvolupar el projecte.

Hi haurà reunions cada quinze dies amb el director, el professor Josep Solé, un doctorand i quatre estudiants que estan realitzant un projecte similar. Aquestes reunions tenen una duració de dues hores.

La persona encarregada de desenvolupar el projecte dedicarà com a mínim 30 hores setmanals.

7.2 Recursos hardware

1) *Portàtil Acer e-1572*. Ordinador personal on es desenvoluparà gran part del projecte, amb dos sistemes operatius, Windows 10 i Ubuntu 16.04 .

2) *Conexió a internet mitjançant el router*. Permetrà connectar-se a internet per accedir a les pàgines que s'analitzaran.

7.3 Recursos software

1) *Ganttter*. Eina per crear diagrames de Gantt.

2) *Correu electrònic Gmail*. Eina de comunicació amb el director.

3. *Sublime Text*. Editor de textos per escriure i visualitzar el codi que es crearà. Aquesta eina serà utilitzada per desenvolupar la eina.

4. *Google Chrome*. Navegador web que servirà per executar les pàgines web que s'analitzaran.

4. *Selenium WebDriver* [13] . Eina utilitzada per la automatització de crides al navegador web.

8. Valoració d'alternatives i pla d'acció

En l'execució d'aquest projecte poden sorgir eventuais desviacions.

En la fase de recerca hi ha un risc de desviació, ja que es possible que es trobi un treball semblant a aquest utilitzant la mateixa estratègia de detecció. En cas que fos així s'hauria de desviar el projecte per tal de diferenciar-lo. Això afectaria poc en la duració del projecte. Es necessitarà l'ajuda del director per guiar al desenvolupador. L'afectació en la duració seria d'un parell de dies.

En la fase de desenvolupament hi ha un risc de desviació alt, ja que el desenvolupador haurà de treballar amb noves tecnologies que poden arribar a causar desviacions importants en la duració d'aquest projecte. Els recursos necessaris per afrontar aquesta desviació serien més temps de desenvolupament i aprenentatge del desenvolupador. Podria fer augmentar el temps de duració de la tasca de desenvolupament una setmana més.

Encara que hi hagi una desviació es poden utilitzar dues setmanes per solucionar-ho.

L'altra alternativa seria reduir la fase de mesurament, fent una comparació més simple amb els altres estudis i eines.

Amb aquestes solucions i amb la metodologia utilitzada que redueix la probabilitat de riscos s'assegura acabar el treball de fi de grau en el temps previst encara que sorgeixin desviacions temporals.

9. Desviació de la planificació

La planificació ha sofert un canvi que ja s'havia tingut en compte en la valoració d'alternatives. Aquest canvi ha sigut provocat per la restriccions de seguretat que tenen els navegadors. Per solucionar-ho han calgut dues setmanes més de feina. Els costos d'aquesta desviació han sigut coberts pels costos d'imprevistos i contingència. L'augment del cost ha sigut de 438€. (40 hores del programador, 2 setmanes de recusus indirectes).

9. Autoavaluació de la competència de sostenibilitat

En el transcurs del grau se'ns ha avaluat en les competències de sostenibilitat i compromís social de forma genèrica, però amb l'ajuda del qüestionari he pogut identificar els meus punts forts i febles en aquesta competència. Se fer un anàlisi sistemàtic i crític de la situació global, també sóc capaç d'identificar els causes d'un problema i les possibles conseqüències. Però em costa relacionar-ho amb problemes similars i solucions ja efectuades.

En la part d'innovació, conec i comprenc les tècniques d'innovació i de generació d'idees, com la coneguda pluja d'idees (*brainstorm*). A més a més, sóc capaç aportar noves idees per fer els projectes més sostenibles.

En l'impacte ambiental, comprenc el cost ambiental dels productes que creem, encara que em costa fer un anàlisi crític de l'impacte que pot provocar al llarg de la seva vida útil. Però també cal recalcar que tinc en compte els efectes ambientals en els projectes que efectuo. Seria capaç de proposar un projecte sostenible, tenint en compte els aspectes ambientals, socials i econòmics. Conec el paper estratègic que tenen les TIC en la sostenibilitat, justícia social i economia circular.

A més a més, tinc en compte els problemes d'accessibilitat, ergonomia i seguretat dels productes i projectes TIC. Però em costa entendre la problemàtica amb la justícia social i l'equitat. Tinc clar les conseqüències directes i indirectes que poden causar els serveis i productes TIC, també sé valorar el grau d'accessibilitat, ergonomia i seguretat del producte o servei. Se fer una valoració de si un producte està fent un bé comú a la societat, encara que en els projectes que he realitzat no he inclòs una estimació per estimar la contribució de millora a la societat. Em costa realitzar la gestió econòmica d'un producte o servei al llarg de la seva vida útil. En els projectes que he realitzat s'ha utilitzat eines de treball col·laboratiu, i les metodologies que s'efectuen en treballs en grup.

10. Gestió econòmica

10.1 Costos de recursos humans

El projecte serà realitzat només per una persona, però efectuarà els rols de project manager, analista, programador, tester i documentador en el transcurs del projecte.

Els salaris de cada rol són orientatius,

A continuació es defineixen les tasques que efectuaran els diferents rols de les diferents fases del diagrama de Gantt.

Project manager. Serà l'encarregat de definir i planificar el projecte, és a dir, la fase de planificació.

Analista. Realitzarà la funció de disseny de l'eina, escollint les tecnologies necessàries per ser implementada.

Programador. Efectuarà el desenvolupament de l'eina, és a dir la fase de desenvolupament.

Tester. Realitzarà la fase de comprovació de l'eina.

Científic de dades. S'encarregarà d'executar l'eina, analitzar els resultats i comparar-los amb treballs relacionats, és a dir, la fase de mesurament.

Documentador. Realitzarà tota la documentació del projecte.

Rol	Hores estimades	Preu per hora (€/h)	Cost estimat (€)
Project manager	110	15.38	1691.8
Analista	90	20.31	1827.9
Programador	140	10	1400
Tester	20	8	160
Científic de dades	60	12	720
Documentador	60	8	480
Total	480		6279.7

Taula 3. Estimació dels costos de recursos humans per rol

10.2 Costos de recursos materials

Per realitzar aquest projecte cal utilitzar recursos hardware i software que tenen un cost associat.

En l'apartat de hardware es troba el material físic necessari per realitzar l'eina. S'utilitzarà un portàtil Acer amb sistema dual (Ubuntu 16.04, Windows 10). El cost del sistema operatiu Windows ve inclòs amb l'ordinador.

En l'apartat software es troba el programari utilitzat per desenvolupar el projecte. Tot el programari utilitzat és OpenSource o té una versió reduïda gratuïta. Per tant, no hi han costos relacionats amb el software.

Per últim ens trobem amb el cost d'impressió de la memòria. Es faran còpies per cada professor del tribunal. El cost d'impressió en color és de 0.50 €/full, a més a més s'enquadrarà[14].

Producte	Unitats	Vida útil (anys)	Cost(€)	Amortització (€)
Acer Aspire e1572	1	6	500	28
Còpies de la memòria	3		30	
Total			530	28

Taula 4. Estimació dels costos de recursos hardware per producte.

10.3 Costos indirectes

El cost indirecte afecta al procés productiu però no es pot assignar de manera directa a un producte. Aquests costos són els de l'electricitat, l'aigua, el transport, el lloguer del pis, el gas, i l'internet durant el transcurs del projecte(4 mesos).

Servei	Preu (€/mes)	Cost estimat (€)
Electricitat	40	160
Aigua	30	120
Transport	50	200
Lloguer	300	1200
Gas	30	120
Internet	36	144
Total	486	1944

Taula 5. Estimació dels costos indirectes

10.4 Contingència

Es reservarà un 10% dels costos totals per si hi ha una variació de la planificació que afecti el cost del projecte. El nivell de contingència assignat és baix degut als pocs riscos de desviació que s'han analitzat prèviament.

Costos	Percentatge (%)	Cost	Contingència(€)
Recursos Humans	10	6279.7	627.97
Recursos Materials	10	530	53
Indirectes	10	1944	194,4
Total			875.37

Taula 6. Estimació de la contingència

10.5 Imprevistos

Com ja s'ha esmentat en el pla d'acció poden sorgir imprevistos que afectin la durada del projecte. En el desenvolupament del projecte es pot trobar amb els següents imprevistos:

El primer imprevist és que el desenvolupador tardi més en implementar l'eina (1 setmana), cosa que és probable ja que es treballa amb noves tecnologies (s'assigna un 40% de probabilitat).

El segon imprevist pot ser causat per la necessitat de més recursos hardware per executar l'eina implementada en les pàgines més visitades (s'assigna un 20% de probabilitat). Per contrarestar aquest imprevist es pot utilitzar els servidors de Microsoft Azure (8 CPU, 16 RAM durant 30 h)[15].

Per últim, l'ordinador pot avariar-se durant el transcurs del desenvolupament de l'eina, això pot afectar molt el temps de duració del projecte si es decideix reparar-lo en el servei tècnic. Per tant la millor solució seria comprar un altre ordinador (s'assigna un 10% de probabilitat).

Producte	Probabilitat (%)	Temps (h)	Preu	Cost (€)
Imprevist desenvolupament	40	30	8€ / h	240
Necessitat de recursos hardware	20	30	76 €	76
Averia ordinador	10		500 €	500
Total				816

Taula 7. estimació dels imprevistos

10.6 Pressupost final

Per finalitzar, s'agrupen tots els costos totals per desenvolupar el projecte en la següent taula.

RRHH	Materials	Indirectes	Contingència	Imprevistos	Total
6279.7€	530€	1944€	875.37€	816€	10445.07€

Taula 8. estimació del pressupost final

10.7 Control de gestió

En el transcurs del projecte poden sorgir desviacions que seran contingudes pel pla d'acció i la planificació establerta.

El mecanisme que s'utilitzarà serà el d'avaluar els costos una vegada acabada cada fase per determinar els costos reals i els que s'han estimat en la planificació.

La comparació dels costos reals i estimats no ha de ser gran, en cas que existeixi una diferència alta s'haurà d'analitzar la causa per intentar minimitzar-ho en les altres fases.

Si la suma dels costos reals supera als estimats s'hauria d'utilitzar el pla de contingència estudiat anteriorment que permet un nivell de contingència del 10% per cobrir els costos totals.

Amb això es té garantit l'aplicació del projecte encara que es produeixin imprevistos que afectin la duració i cost d'aquest.

11. Sostenibilitat i compromís social

11.1 Dimensió econòmica

PPP

En l'apartat de costos es fa una avaluació detallada dels recursos humans, materials i indirectes necessaris per realitzar el projecte de forma estimada. En l'avaluació s'observa que el 49,47% dels costos provenen dels recursos humans. Per tal de reduir els costos, seria necessària reduir el temps de treball de l'enginyer, això només seria possible si l'enginyer tingués experiència prèvia en les tecnologies que s'utilitzaran al llarg del projecte.

La resta de costos són inevitables, ja que existeixen encara que no es tingui que realitzar el projecte.

Actualment, les eines existents tenen poca eficàcia en la detecció del minat de criptomonedes. L'objectiu d'aquest projecte és detectar de forma eficaç el minat de criptomonedes, amb això els usuaris finals tindrien un estalvi econòmic significant.

Per reduir el cost del projecte s'ha procedit a reutilitzar codi d'un TFG que estudiava l'ús del *web tracking* [16]. Això a permès reduir una setmana de feina ja que només s'ha reutilitzat la base del codi. L'estalvi ha sigut de 200€ (20h del programador*10€).

Aquest projecte ha tingut un imprevist que ja estava considerat en els possibles imprevistos. Ha calgut dues setmanes de feina del treballador, això ha sigut contingut pels costos guardats per possibles imprevistos. El cost del imprevist ha sigut de 438€. El cost final del projecte ha sigut de 9191,7€. Hi ha hagut un estalvi del 12% respecte el pressupost inicial, ja que no ha sigut necessari l'ús de tota la part de costos d'imprevistos i contingència.

Vida útil

El cost principal de la vida útil d'aquest projecte depèn dels canvis que hi hagi en la mineria de criptomonedes en les pàgines web. En cas que hi hagi un canvi major en la mineria de criptomonedes, com pot ser la encriptació dels paquets WebSocket, s'hauria de replantejar el mètode de detecció.

En cas que es mantingui la mineria de criptomonedes tal i com és, el cost de manteniment de l'eina és molt baix. El cost estimat de manteniment anual és del 10% del cost del projecte, és a dir 919,17€.

Riscos

Com s'ha comentat en l'apartat anterior, el risc principal és el d'un canvi significatiu en la mineria de criptomonedes en les pàgines web. Actualment és necessari l'ús dels WebSockets per minar, però potser que els navegadors treguin una API més eficient per comunicar-se amb els servidors de minat. En aquest cas hi hauria un sobrecost de modificació en l'eina per seguir detectant-ho.

11.2 Dimensió ambiental

PPP

L'impacte ambiental de l'estudi que es realitzarà es baix, ja que els recursos materials necessaris per la realització del projecte ja existien abans. Per tant, només s'utilitzarà energia elèctrica en l'àmbit ambiental per l'execució de l'eina desenvolupada.

A més a més, amb la detecció de les pàgines de minat de criptomonedes es reduiria de forma significant l'energia utilitzada en els dispositius reduint l'ús de la CPU.

Els recursos que afecten a l'àmbit ambiental no poden ser reduïts, ja que són costos indirectes que existeixen encara que no s'hagués de fer el projecte. També s'utilitzarà un ordinador que ja porta anys en ús, per tant s'està reciclant un recurs ja existent.

S'utilitzarà recursos software ja existents per reduir el temps d'execució del projecte.

Per finalitzar, aquest estudi ajudarà en futures recerques en aquest àmbit reduint la petjada ecològica.

Aquest projecte només es podria fer amb menys recursos si l'autor tingués coneixements amplis sobre el tema. Així es reduiria el temps d'execució d'aquest projecte.

A continuació es mostrarà l'estimació de recursos ambientals que consumirà el projecte en 4 mesos.

Principalment aquest projecte necessita d'un ordinador i una persona que s'encarregui de fer l'eina.

Activitat	Consum per hora (Kw/h)	Consum total (Kw)	Petjada (Kg de CO ²)
Treballador	0,1	48	17,76
Portàtil	0,125	60	22,20
Total	0,225	108	39,96

Taula 9. Estimació del consum de les activitats del projecte

Vida útil

A continuació es mostrarà l'estimació de recursos ambientals que consumirà el projecte en la seva vida útil.

Principalment aquest projecte necessita d'un ordinador i una persona que s'encarregui de fer el manteniment de l'eina.

Activitat	Consum per hora (Kw/h)	Consum total (Kw)	Petjada (Kg de CO ²)
Treballador	0,1	36	13,32
Portàtil	0,125	45	16,65
Total	0,225	81	29,97

Taula 10. Estimació anual del consum de la vida útil del projecte

L'eina desenvolupada pot permetre una reducció significativa del consum d'electricitat global, ja que permet detectar pàgines que utilitzen l'electricitat dels dispositius per minar criptomonedes que necessiten d'un ús excessiu de la CPU.

Riscos

Ambientalment aquest projecte no té riscos que poguessin augmentar la petjada ecològica del projecte. Al contrari, aquest projecte permet reduir la petjada ecològica si s'utilitza l'eina.

11.3 Dimensió social

PPP

A nivell personal, aquest projecte aportarà coneixements en les diferents tecnologies utilitzades i en la seguretat de les pàgines web.

A més a més ajuda a tenir reflexions per tal de poder portar a terme projectes sostenibles.

Els canvis provocats per aquest projecte han sigut positius, ja que s'ha après a portar a terme un projecte tenint en compte aspectes no tant tècnics com la gestió i planificació. L'estudi que es realitza afectarà positivament als usuaris, ja que entendran que poden haver programes en les pàgines web que utilitzen els seus recursos, a més a més, també sabran si una pàgina està utilitzant la CPU per una acció que no han sol·licitat.

Vida útil

Els beneficiaris d'aquest projecte són les organitzacions i usuaris finals que naveguen per internet.

Existeix una necessitat real d'aquest projecte per tal de millorar la qualitat de vida de tots els usuaris que naveguen per internet, ja que la majoria de pàgines web que utilitzen els nostres recursos per minar no ens adverteixen d'aquest ús pel seu benefici.

Les pàgines web poden ser afectades per aquest projecte ja que avisaria que la pàgina web que s'està utilitzant està utilitzant la CPU. Però no és una afectació important ja que es possible utilitzar alternatives per monetitzar el contingut de les pàgines web.

El projecte soluciona el problema plantejat a l'inici detectat de forma efectiva l'ús de la mineria de criptomonedes en pàgines web.

Riscos

Com ja s'ha comentat anteriorment, el principal col·lectiu que es veuria afectat són els propietaris de les pàgines web i tots els treballadors que formen part de la creació, administració i manteniment de la pàgina web. Però aquest projecte no crearia cap tipus de dependència que deixes al col·lectiu esmentat en posició de debilitat, ja que hi ha altres maneres de monetitzar les pàgines web i obtenir millors beneficis.

11.4 Matriu de sostenibilitat

En la taula següent es mostra la puntuació de la sostenibilitat d'aquest projecte d'acord amb les valoracions fetes en els punts anteriors.

	PPP	Vida útil	Riscos
Ambiental	39,96 Kg de CO ²	29,97 Kg de CO ² /anual	2
Econòmic	9191,7€	919,17€	6
Social	7	8	5

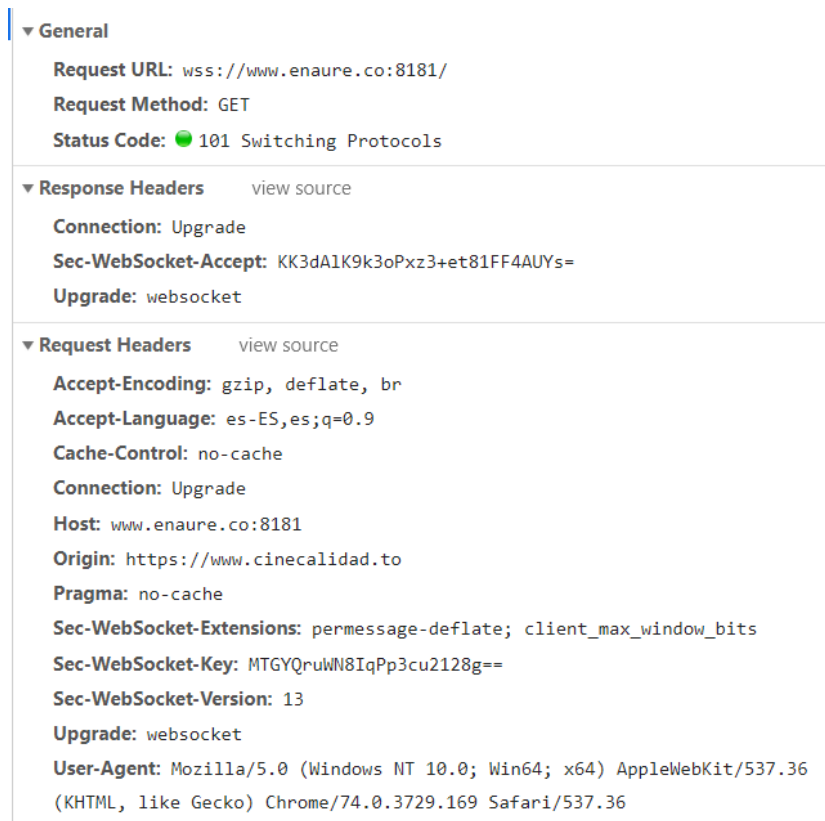
Taula 11. Valoració de la sostenibilitat

12. Anàlisi del cryptojacking

Per trobar un mètode de detecció ha calgut analitzar diverses pàgines que utilitzen el minat de criptomonedes.

12.1 HTTPS

En la primera fase d'anàlisi, amb l'ajuda del desenvolupador web del navegador Chrome, s'ha analitzat el tràfic HTTPS per observar si hi ha alguna coincidència entre les pàgines de minat en les peticions i respostes. Amb aquesta opció s'ha pogut detectar que per la interacció entre el servidor de minat (*mining pool*) i el navegador s'obre un WebSocket.



The screenshot shows the Chrome DevTools Network tab with a selected request. The 'General' tab is active, displaying the following details:

- Request URL:** wss://www.enaure.co:8181/
- Request Method:** GET
- Status Code:** 101 Switching Protocols

Below the general information, the 'Response Headers' and 'Request Headers' are expanded:

Response Headers:

- Connection:** Upgrade
- Sec-WebSocket-Accept:** KK3dA1K9k3oPxz3+et81FF4AUYs=
- Upgrade:** websocket

Request Headers:

- Accept-Encoding:** gzip, deflate, br
- Accept-Language:** es-ES,es;q=0.9
- Cache-Control:** no-cache
- Connection:** Upgrade
- Host:** www.enaure.co:8181
- Origin:** https://www.cinecalidad.to
- Pragma:** no-cache
- Sec-WebSocket-Extensions:** permessage-deflate; client_max_window_bits
- Sec-WebSocket-Key:** MTGYQruWN8IqPp3cu2128g==
- Sec-WebSocket-Version:** 13
- Upgrade:** websocket
- User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36

Figura 2 Pàgina cinecalidad.to on es visualitza l'ús del websocket

12.2 Codi font

En la segona fase, s'ha procedit a fer enginyeria inversa analitzant el codi font de minat de criptomonedes de diverses pàgines web. Alguns dels codis fonts estan ofuscats, és a dir el codi s'ha modificat perquè no sigui comprensible per una persona.

```
var _0x550789 = _0x5dad4c(this, function() {  
    var _0x2afc29 = function() {  
        return '\x64\x65\x76';  
    }  
    , _0x2b3b95 = function() {  
        return '\x77\x69\x6e\x64\x6f\x77';  
    }  
});
```

Codi 1 Codi obfuscat de la pàgina thepiratebay

S'ha observat que el codi font depèn de la moneda que s'està minant i la plataforma que ha generat el codi font. Les dues criptomonedes més utilitzades per minar en pàgines web són *Monero* i *JSECoin*.

Monero

Monero és una criptomoneda de codi obert creada al 2014, que es diferencia per la privadesa i la descentralització[17]. Utilitza el protocol de prova de treball *CryptoNight*. Aquest protocol permet que s'executi en dispositius de propòsit general. Només utilitza la CPU a diferència d'altres protocols que utilitzen la GPU com el protocol de *Bitcoin*[18].

En el codi s'ha pogut observar que per aquesta criptomoneda s'utilitza WebAssembly i WebWorkers.

JSEcoin

JSEcoin es va llençar el juliol de 2018. Aquesta criptomoneda ha estat creada específicament per ser minada en les pàgines web. S'utilitza l'algoritme de hash SHA256 (Elliptical curve secp256k1)[19], això permet que es pugui minar amb qualsevol dispositiu de propòsit general. A diferència d'altres serveis, en accedir a la pàgina web s'obre una notificació que adverteix de l'ús de la CPU.

12.3 Tipus d'execucions

Hi ha dues formes d'executar el codi de minat:

1. La primera forma consisteix en afegir codi Javascript en l'arxiu índex de la pàgina. Aquest codi està en el domini de la pàgina que s'ha accedit, això dificulta. En el codi següent hi ha la adreça en hexadecimal de la pàgina per ser identificada pel servei que ha ofert el codi. S'observa que el servei que proporciona el codi és *CRyptoLooT*. També hi ha informació sobre els fils d'execució que s'utilitzaran i l'ús màxim de la CPU(throttle). L'execució del codi es fa des del codi HTML.

```
var miner=new CRLT.Anonymous('cb8605f33e66dcef8735d485091065495494d',{
  threads:4,autoThreads:false,throttle:0.2
});
if (!miner.isMobile()) {
  miner.start();
}
```

2. La inserció del codi es fa afegint l'origen del codi Javascript que sol estar en un domini diferent al de la pàgina.

```
<script>
  if (!(/TV/i.test(navigator.userAgent))) {
    var r2d2 = document.createElement('script');
    r2d2.src = 'https://www.enaure.co/javas.js?v=2';
    r2d2.setAttribute('defer', 'defer');
    document.getElementsByTagName('head')[0].appendChild(r2d2);
  }
</script>
```

12.4 Detecció

Anteriorment s'han esmentat tecnologies utilitzades per la mineria de criptomonedes que s'han trobat en l'anàlisi HTTPS i el codi font, aquestes tecnologies són les següents.

WebSocket

El WebSocket és una tecnologia avançada que proporciona una comunicació bidireccional i full-duplex. Permet obrir una sessió de comunicació interactiva entre un client i servidor. Amb aquesta API es pot enviar missatges a un servidor i rebre respostes controlades per events sense tenir que consultar al servidor per una resposta.

Els WebSockets s'utilitzen en serveis on es cal una actualització real en temps real. Per exemple, pàgines web de xarxes socials, videojocs online i pàgines amb informació de la borsa de valors.

WebAssembly

Algun dels codis com el del servei *Coinhive* i *Cryptoloot* utilitzen una nova característica del navegador anomenada *WebAssembly*, aquest és un nou tipus de codi en assemblador en format binari que s'executa en els navegadors. El propòsit és poder executar codi d'altres llenguatges de programació com C, C++ o Rust en les pàgines web amb un rendiment superior al codi Javascript. Aquesta tecnologia permet millorar el hash rate de la mineria augmentant els beneficis de les pàgines web. Aquesta tecnologia no es utilitzada en tots els codis de minat, per exemple JSECoin no l'utilitza.

WebWorkers

Aquesta tecnologia permet executar un codi Javascript en un fil d'execució diferent al de la pàgina web. El propòsit és executar tasques computacionalment laborioses sense interrompre la interfície d'usuari d'una pàgina web.

Objecte Window

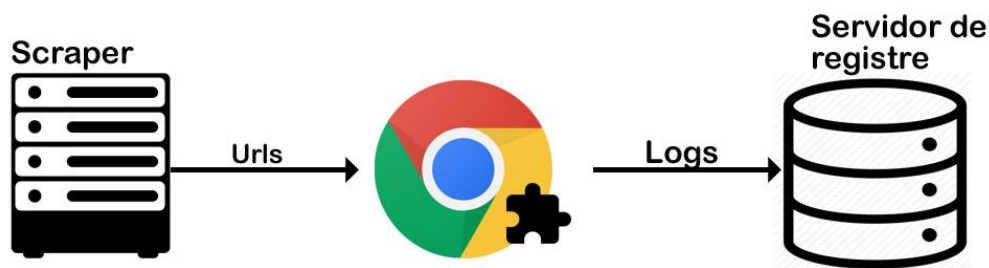
El window representa un objecte que conté el document DOM⁴ de la pàgina web. Tots els objectes, funcions i variables globals de Javascript pegen del objecte window. En el cas del codi de minat també penjarà del objecte window, per tant es podrà detectar registrant aquest objecte.

⁴ És una API per a documents HTML i XML, proporciona una representació d'una pàgina web.

13 Disseny i implementació

Per a la detecció del minat en les 100.000 pàgines web més visitades segons el rànquing d'Alexa, s'utilitza principalment els WebSockets, WebWorkers i l'objecte Window de la DOM.

El programa consisteix en una extensió que s'executarà mitjançant el servidor scraper. Aquesta extensió s'encarregarà de registrar les crides Javascript que posteriorment s'enviaran al servidor de registre. Una vegada finalitzada l'execució s'utilitzarà un analitzador per verificar l'ús de mineria de criptomonedes amb les dades dels registres.



1. Esquema de l'eina

13.1 Servidor scraper

El servidor scraper utilitza el WebDriver de Selenium per executar el navegador Chrome amb l'extensió de registre. El WebDriver permet automatitzar l'accés a les pàgines web del navegador Chrome. Aquest servidor, una vegada inicialitzat el navegador i instal·lada l'extensió, navega per un fitxer amb el rànquing de pàgines i obre les pàgines.

El codi permet l'execució de diferents scrappers alhora per tal de paral·lelitzar l'anàlisi de pàgines. En els arguments de l'execució s'indica les pàgines que es vol analitzar segons el rànquing.

```
def main():
    args = parser.parse_args()
    sites = config.load_alexas_csv(args.filename)[slice(args.start,
args.end, None)]
    driver = build_chrome()
    driver.set_page_load_timeout(20)
    for rank, site in enumerate(sites, args.start + 1):
        try:
            visit_site(driver, rank, site)
        except TimeoutException:
            print('timed out')
            driver.quit()
            driver=build_chrome()
            driver.set_page_load_timeout(20)
```

Codi 2 Scraper. Accés a les pàgines

13.2 Extensió

La extensió s'encarrega de registrar les crides a la API *WebSocket*, *WebWorker*. Això s'aconsegueix utilitzant el mètode *Monkey Patch*. Aquest mètode consisteix en afegir funcionalitats a una funció sense modificar el seu codi original. Per a l'obtenció de l'objecte window per obtenir una millor lectura s'eliminaran les funcions que venen per defecte del navegador.

WebSocket

Es modificarà el constructor del *WebSocket* per registrar el url i el protocol. Amb aquesta funció es podrà identificar el domini de mineria. Per registrar la informació que s'envia i es rep del *WebSocket* es procedirà a registrar la funció *send*.

```
WebSocket WebSocket(  
    in DOMString url,  
    in optional DOMString protocols  
);  
WebSocket.send(data);
```

Codi 3 Funció constructora i d'enviar del WebSocket

WebWorker

En la API del *WebWorker* es procedirà a modificar dues funcions. La funció constructora servirà per registrar el codi que s'especifica al *URL*. Aquest codi s'envia del fil d'execució principal de la pàgina cap al *worker* que s'acaba de generar perquè l'executi. La segona funció registrarà els missatges que s'envien i reben del *worker*.

```
WebSocket WebSocket(  
    in USVString aurl,  
    in optional DOMString options  
);  
worker.postMessage(message);
```

Codi 4 Funció constructora i d'enviar del WebWorker

Totes aquestes funcions s'han modificat perquè afegixen la funcionalitat de registrar informació per ser enviada al servidor de registre mitjançant la extensió. El missatge s'envia com a fitxer JSON mitjançant el protocol HTTP amb la API XMLHttpRequest del navegador.

```
function sendtoServer(param) {  
    var xhr = new XMLHttpRequest();  
    xhr.open("POST", "http://127.0.0.1:8080/", true);  
    xhr.setRequestHeader("Content-Type", "application/json");  
    console.log('before sending the request');  
    xhr.onload = function() {  
        if(xhr.readyState == 4 && xhr.status == 200) {  
            console.log('Send with status 200');  
        }  
    }  
}
```

```

    }
  }
  xhr.onerror = function() {
    console.log('There was an error!');
  };
  xhr.send(JSON.stringify(param));
}

```

Codi 5 Funció per enviar dades al servidor

Objecte Window

Per a l'obtenció del window es crearà un nou objecte per filtrar les funcions que venen per defecte del navegador. Amb aquest mètode s'obtingueran les funcions obtingudes de la pàgina web per tractar-les posteriorment.

```

iframe = document.createElement('iframe');
iframe.style.display = 'none';
document.body.appendChild(iframe);
currentWindow = Object.getOwnPropertyNames(window);
results = currentWindow.filter(function(prop) {
  return !iframe.contentWindow.hasOwnProperty(prop);
});
document.body.removeChild(iframe);

```

Codi 6 Filtratge de l'objecte window

13.3 Servidor de registre

El servidor de registre s'encarrega principalment de rebre i tractar els registres enviats per la extensió. El servidor rep els missatges mitjançant el mètode POST del protocol HTTP i emmagatzema en una base de dades SQLite.

Aquest servidor necessita encarregar-se de moltes peticions alhora que provenen del scrappier. Per resoldre-ho es crearan workers mitjançant gunicorn que gestionaran les peticions[20].

La taula següent s'omple en iniciar el servidor amb un arxiu de les pàgines web més populars segons el rànquing d'Alexa.

Variable	Tipus	Descripció
Id	Integer	Identificador únic
Domain	Integer	Nom de la pàgina web
Alexa_rank	Integer	Posició en el rànquing segons Alexa

Taula 12 Base de dades del Domini

Una vegada iniciat la base de dades del domini es procedeix a obrir el port 8080 de *localhost* per rebre dades de l'extensió.

L'extensió envia un registre de cada pàgina de la taula següent. Si la pàgina utilitza *WebSockets* el registre s'actualitzarà amb l'adreça iniciada , i si s'inicia un *WebWorker* s'actualitzarà amb el script que es passa al *Worker*.

En cas que la pàgina no utilitzi *WebSockets* o *WebWorkers* les variables *script* i *address* estaran buides.

Variable	Tipus	Descripció
Id	Integer	Identificador únic
Domain_id	Integer	Identificador de la taula Domain
Measured_At	Datetime	Data de la mesura
Window	String	L'objecte window
Script	String	Codi enviat al Worker
Address	String	Adreça del WebSocket

Taula 13 Base de dades del Registre

L'extensió envia un registre de la taula següent quan la pàgina envia o rep missatges del *WebSocket*.

Variable	Tipus	Descripció
Id	Integer	Identificador únic
Domain_id	Integer	Identificador de la taula Domain
Sent	Datetime	Boolea que indica si s'envia o es rep el missatge
Message	String	Missatge enviat o rebut del WebSocket
Stack	String	Pila d'execució

Taula 14 Base de dades del WebSocket

La taula següent serveix per emmagatzemar els missatges enviats i rebuts del *WebWorker*.

Variable	Tipus	Descripció
Id	Integer	Identificador únic
Domain_id	Integer	Identificador de la taula Domain
Message	String	Missatge enviat o rebut del Worker
Stack	String	Pila d'execució

Taula 15 Base de dades del WebWorker

13.4 Analitzador

L'analitzador utilitza les bases de dades per filtrar les pàgines de mineria de dades. El programa consisteix en una sèrie de paraules clau que són buscades en les taules. Aquest programa es necessari ja que hi ha altres pàgines web que utilitzen *WebSockets* o *WebWorkers* per altres usos com el *streaming* o jocs online.

14. Seguretat

El navegador té una capa de seguretat amb la finalitat de protegir les dades y evitar la descàrrega de programes maliciosos. La eina creada necessita enviar dades de la pàgina web visitada cap al servidor que esta en un domini diferent de la pàgina. Aquesta acció no es possible sense la modificació del servidor perquè es bloqueja amb la mesura CORS del navegador. A més a més el navegador té una política anomenada CSP que bloqueja l'execució de certes funcions.

14.1 CORS

L'intercanvi de Recursos d'Origen Creuat (CORS) és un mecanisme que utilitza capçaleres HTTP addicionals per permetre que un *user agent*⁵ obtingui permisos per accedir a recursos seleccionats des d'un servidor en un domini diferent[21]. Per permetre aquesta política s'han afegit capçaleres al servidor perquè accepti qualsevol petició del navegador.

```
def _enable_cors(*args, **kwargs):
    response.headers['Access-Control-Allow-Origin'] = '*'
    response.headers['Access-Control-Allow-Methods'] = 'GET, POST,
PUT, OPTIONS'
    response.headers['Access-Control-Allow-Headers'] = 'Origin,
Accept, Content-Type, X-Requested-With, X-CSRF-Token'

    if bottle.request.method != 'OPTIONS':
        return fn(*args, **kwargs)
```

```
return _enable_cors
```

Codi 7 Activació del CORS en el servidor

14.2 CSP

La Política de Seguretat del Contingut(CSP) és una capa de seguretat que detecta i evita atacs d'injecció de codi, com per exemple el tipus de vulnerabilitat informàtica XSS (cross site scripting), que permet inserir codi que l'executa el client en una pàgina. Amb aquesta vulnerabilitat es pot obtenir les credencials d'una pàgina web. En l'eina desenvolupada s'injecta codi Javascript en les pàgines web i s'envia les dades mitjançant HTTP. La pàgina web si té configurada aquesta política detecta l'eina com una amenaça i bloqueja la funció *XMLHttpRequest* que permet enviar les dades al servidor. Per evitar aquest bloqueig en el navegador Chrome es necessària la desactivació d'aquesta política que es pot fer mitjançant la extensió *Disable Content-Security-Policy* [22]. Aquesta extensió s'ha modificat per inserir-se en el servidor *scraper* i activar-se

⁵ És un identificador únic del dispositiu creat a partir d'informació del hardware i software.

automàticament. El *scraper* s'encarregarà de instal·lar-la juntament amb l'extensió de registre de les pàgines.

15. Proves de validació

Per validar l'eina creada s'utilitzarà una llista de pàgines detectades per la pàgina NotMining que proporciona una llista negra amb pàgines que utilitzen o han utilitzat mineria de criptomonedes[23]. Encara que moltes d'aquestes pàgines no són accessibles o no segueixen utilitzant el minat de criptomonedes, ja que la llista negra no està actualitzada.

A continuació es mostren les dades que s'han registrat amb el programa creat.

15.1 Registres

WebSocket

L'eina ha interceptat les comunicacions del WebSocket, en la figura següent es pot veure l'exemple d'una comunicació de mineria de criptomonedes. S'observa que hi ha l'adreça de la pàgina per identificar-la en el servidor, així el treball realitzat per l'usuari serà remunerat a la cartera ⁶ de la pàgina web. El paquet indica la criptomoneda que es minarà (XMR- Monero). S'utilitza un cercador de paraules clau per filtrar pàgines web que utilitzen WebSockets però no fan mineria.

```
{ "type": "auth",  
  "params":  
    { "site_key": "cb8605f33e66d9d52524cef8735d485091065495494d",  
      "type": "anonymous",  
      "user": null,  
      "goal": 0,  
      "version": 3000, "  
      "coin": "xmr" } }
```

Figura 3 Paquet WebSocket amb informació de mineria de criptomonedes.

⁶ Wallet, és una cartera virtual encriptada on s'emmagatzemen les criptomonedes dels usuaris.

WebWorker

En la següent figura es mostra un missatge de mineria enviat del fil d'execució principal cap a un *worker*. En ell es mostra el blob que indica l'identificador del bloc que es vol minar que prové del servidor de minat. El missatge també indica l'algoritme que s'utilitza que en aquest cas és el *CryptoNight(cn)* i el llimitar màxim d'ús de la CPU que és de 80% (throttle).

```
{ "job": { "blob": "0b0beaf798e805905872ee40c48a290477eb3ae5a2f64207657cc16aa533a8a73b6820d3b3b65d00000000a142244d3774c80cedd17998b3647b8d698a9261f5393d88007e38b15220668c02", "job_id": "pBBYZ9TOFkcRb3zc9v33jU5caTuk", "target": "ffffff01", "id": "05ba3ba1-7afb-44e9-88ad-11321295e604", "algo": "cn", "variant": "4", "height": 1858158 }, "throttle": 20 }
```

Figura 4 Missatge enviat del fil d'execució principal d'una pàgina a un worker

Objecte Window

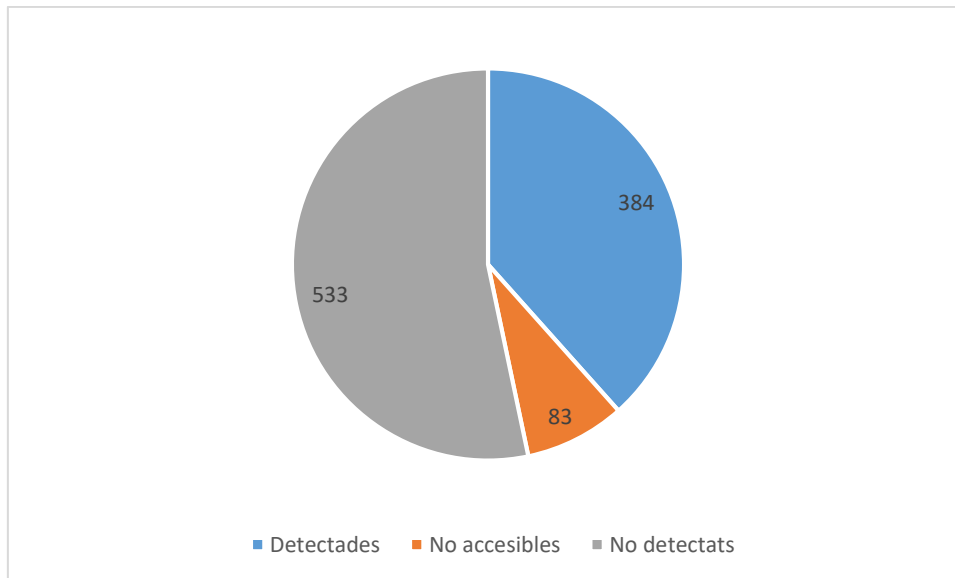
L'objecte *window* existeix en totes les pàgines web, per tant de les pàgines que s'analitzaran sempre es registrarà l'objecte *window* en la base de dades a diferència del *WebSocket* i *WebWorker*. En la següent figura es mostra els mètodes i objectes del *window* una vegada filtrat. El filtrat evita registrar els mètodes i objectes que estan per defecte en totes les pàgines web. S'observa que hi ha un mètode anomenat *FuckAdBlock* injectat en la pàgina web. Aquest mètode fa inservibles l'extensió de bloquejar publicitat *Adblock*. Respecte la mineria de dades també s'observa que hi dos objectes el CRLT que és un objecte del servei *CryptoLoot* i l'objecte miner que és l'encarregat d'executar el codi de minat.

```
[ "GoogleAnalyticsObject", "ga", "google_tag_data", "gaplugins", "gaGlobal", "gaData", "NaConf", "asgPopunder", "_NA", "Base", "__NA", "NA", "asgpjscnf", "FuckAdBlock", "fuckAdBlock", "_0x33e0", "_0x476a", "CRLT", "miner" ]
```

Figura 5 Mètodes i variables de l'objecte window

L'eina s'ha executat amb 4 scrappers per millorar el temps d'execució i paral·lelitzar la feina de les 1000 pàgines. Cada scrapper ha analitzat 250 pàgines web i el temps transcorregut en cada pàgina per analitzar-la ha sigut de 10 segons. Es necessari tindre 4 workers en el servidor per encarregar-se de les peticions HTTP que s'envien de l'extensió. El temps d'execució de les 1000 pàgines ha sigut de 167 minuts.

El percentatge de detecció ha sigut del 8% en 1000 pàgines web visitades. El 39% de les pàgines no eren accessibles.



Gràfic 2 Resultats de l'execució en 1000 pàgines

De les 83 pàgines detectades el 26.5 % es detectat mitjançant el cercador de *keywords* del *WebSocket* i un 32.53 % és detectat mitjançant els *WebWorkers*.

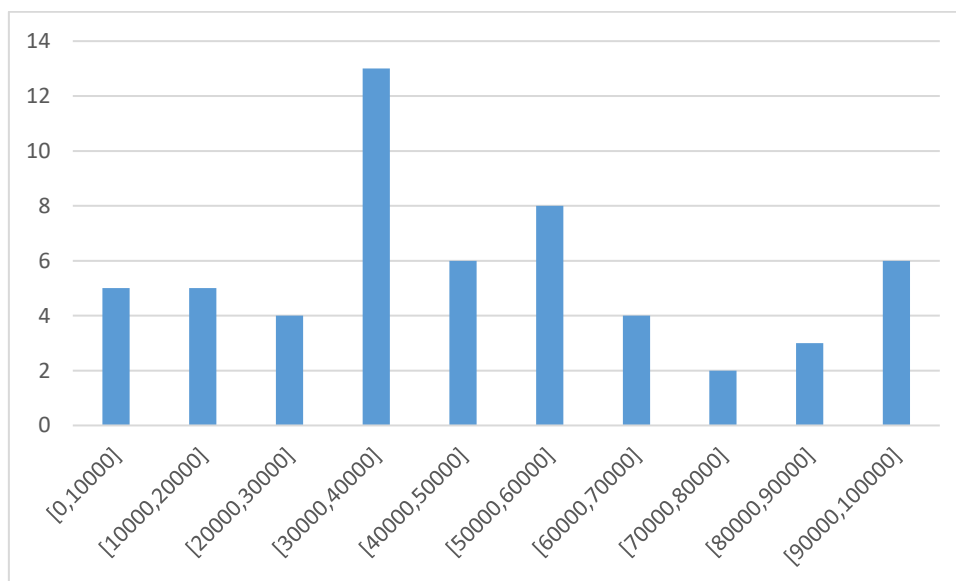
16. Resultats

16.1 Execució

L'eina es executada en les 100.000 pàgines web més populars segons el rànquing d'Alexa. L'execució s'ha fet concurrentment utilitzant 8 workers del scrapper. El temps d'execució ha sigut de 55 hores aproximadament.

25 pàgines s'han detectat mitjançant l'analitzador del WebWorker, 3 pàgines han sigut detectades pel WebSocket i 28 amb l'objecte Window. Sis d'aquestes pàgines han sigut detectades pels 3 mètodes. En general s'han trobat 56 pàgines web en totes les pàgines analitzades amb la metodologia emprada.

En el següent gràfic es mostra el nombre de pàgines web segons la distribució en el rànquing. El 23.2% de les pàgines s'han detectat entre les 30000 i 40000 pàgines web més visitades. S'ha detectat mitjançant l'adreça del WebSocket que 4 de les pàgines estava minant criptomonedes JSECoin. La resta d'adreces és més complicada de detectar ja que les adreces canvien sovint per evitar ser detectats per les extensions existents en els navegadors.



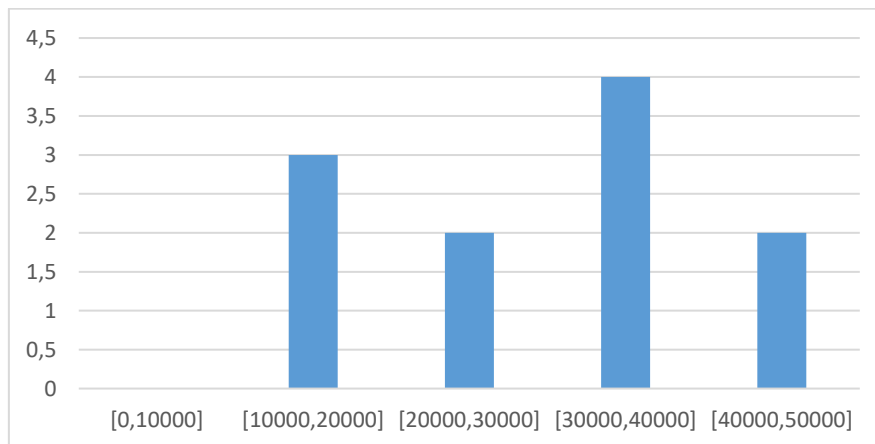
Gràfic 3 Resultats obtinguts de les 100.000 pàgines web segons el rànquing

17. Comparació amb NoCoin

Per fer una comparació real s'ha procedit a modificar l'extensió més popular del mercat per detectar minat de criptomonedes en les pàgines web per afegir-la en el programa. Es procedeix a executar aquesta extensió en les 50.000 pàgines web més populars segons el rànquing d'Alexa automatitzadament.

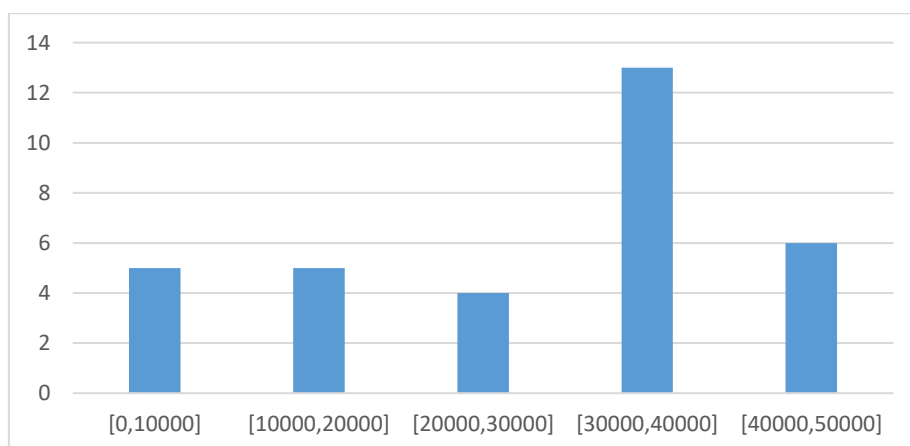
S'han utilitzat 8 scrappers per executar les 50.000 pàgines concurrentment, el temps d'execució ha sigut de 27 hores aproximadament.

L'extensió ha detectat 11 pàgines web en diferents posicions del rànquing com es mostra en el gràfic següent.



Gràfic 4 Resultats de NoCoin segons la posició en el rànquing

L'execució amb l'eina desenvolupada en aquest projecte ha detectat 33 pàgines web. És a dir 22 pàgines web més que l'extensió *NoCoin*. L'eina ha pogut detectar pàgines web fins i tot en les primeres 10.000 pàgines més populars. També s'observa que el rang on s'han trobat més pàgines és el mateix(30000,40000).



Gràfic 5 Resultats de l'eina desenvolupada segons la posició en el rànquing

18. Impacte del Cryptojacking

Una vegada identificades i analitzades les 100.000 pàgines web es procedeix a fer una estimació de l'energia i els beneficis que pot aportar la mineria de criptomonedes. Determinar els beneficis exactes de totes les pàgines web és una tasca que no es trivial ja que els beneficis depenen de molts factors com la popularitat d'una pàgina, el contingut, els dispositius dels visitants i el preu de la criptomoneda. És calcularà els beneficis estimats que pot aportar la mineria en la pàgina més popular que s'ha trobat que és cinecalidad.to. Aquesta pàgina està en el rang 593 i el seu contingut és d'entreteniment. Aquest fet és molt important ja que la mineria de criptomonedes només s'executa mentre és té oberta la pàgina. Cal remarcar que aquesta pàgina no és detectada per l'extensió NoCoin, per tant els càlculs seran més aproximats.

18.1 Consum elèctric

El consum elèctric extra causat per la mineria de dades als usuaris depèn del consum de la CPU, la duració dintre de la pàgina i el total d'usuaris. El càlcul del consum és aproximat ja que el consum de les CPU's dels usuaris es diferent. Per al consum de CPU s'utilitzarà la Intel i5-7400 (65W)[24]. La majoria de codis de minat utilitza més del 50% de la CPU, per tant es considera que l'energia utilitzada en el minat és de 32,5 W. El nombre de visites en el mes de Maig de 2019 (43.63M) i la duració (232s) s'han extret de la pàgina d'anàlisis de pàgines web SimilarWeb[25]. En total, l'electricitat gastada pels usuaris que han accedit a aquesta pàgina durant un dia de maig ha sigut de 3046 KWh. Equival al 87% de l'energia elèctrica anual utilitzada en un habitatge de 3 persones a Espanya[26].

$$E = \text{Consum CPU} \times \text{Duració} \times \sum \# \text{Usuaris}$$

18.2 Benefici

El motiu principal de la mineria de criptomonedes és augmentar la monetització d'una pàgina. Però aquestes pàgines acostumen a utilitzar un servei que els ofereix el codi a canvi d'una comissió. El hash rate utilitzat és el de la CPU intel i5-7400(165 h/s) . la criptomoneda que es mina en la pàgina Cinecalidad.to és Monero. La dificultat és un valor que determina com de difícil serà trobar el *hash* del bloc. La recompensa depèn del valor de la criptomoneda(2.63 XMR)[27]. La comissió depèn del servei, per exemple CryptoLoot té un 12% de comissió. En total , els beneficis diaris de la pàgina cinecalidad són de 44.49€.

$$\text{Benefici} = \frac{\text{Hash Rate} \times (1 - (\frac{\text{Comissió}}{100}))}{\text{Dificultat}} \times \text{Recompensa}$$

19. Integració de coneixements

19.1 Coneixements aplicats

Per a fer aquest projecte eren necessaris coneixements previs que s'han estudiat en les següents assignatures:

- **Base de Dades (BD):** Ha calgut crear bases de dades per registrar les dades del navegador.
- **Xarxes de Computadors (XC):** Conèixer el protocol HTTP i les mesures de seguretat actuals d'aquest protocol.
- **Aplicacions distribuïdes (AD):** Per aplicar el paradigma client-servidor en l'eina.
- **Seguretat informàtica (SI):** Per conèixer els diferents atacs i programes maliciosos que existeixen en les pàgines web.
- **Administració de Sistemes Operatius (ASO):** Per administrar l'execució d'un programa en una màquina virtual mitjançant ssh.
- **Criptografia (C):** Per conèixer com funciona la *blockchain* i els algorismes de *hash*.

19.2 Assoliment de competències

- **CTI2.2: Administrar i mantenir aplicacions, sistemes informàtics i xarxes de computadors.**

Ha calgut administrar l'execució paral·lela de les 100.000 pàgines web en una màquina virtual mitjançant el protocol ssh.

- **CTI3.1: Concebre sistemes, aplicacions i serveis basats en tecnologies de xarxa, tenint en compte Internet, web, comerç electrònic, multimèdia, serveis interactius i computació ubiqua.**

Aquesta competència ha sigut assolida perquè s'ha creat una aplicació per interactuar amb les pàgines web.

- **CTI4: Emprar metodologies centrades en l'usuari i l'organització per al desenvolupament, l'avaluació i la gestió d'aplicacions i sistemes basats en tecnologies de la informació que assegurin l'accessibilitat, l'ergonomia i la usabilitat dels sistemes.**

Es genera una eina paral·lelitzable per analitzar pàgines web que pot ser utilitzada tant per usuaris finals com per empreses o organitzacions.

20. Conclusions

En conclusió, aquest projecte tenia com a objectiu principal fer un estudi sobre el minat de criptomonedes en les 100.000 pàgines més populars segons el rànquing d'Alexa. S'han trobat 55 pàgines diferents utilitzant minat de criptomonedes.

Per la comparació no s'han pogut utilitzar els altres estudis realitzats anteriorment explicats en l'estat de l'art perquè durant aquest any han hagut molts canvis, tant en el valor de la criptomoneda més popular com en els serveis que oferien codi de minat per ser incrustat en les pàgines web. El valor de Monero que és la principal criptomoneda minada en les pàgines web ha caigut un 85%, a més a més s'ha modificat el codi de l'algoritme CryptoNight per minar que ha fet augmentat la dificultat de trobar un bloc.

Un altre factor important ha sigut la tancada del servei que oferia el minat Coinhive, aquest servei tenia el 90,9% del mercat segons Wappalyzer.

Per tant s'ha decidit comparar-ho amb la extensió més popular que existeix anomenada NoCoin. Per la comparació s'ha executat 50.000 pàgines web i només ha detectat 11 pàgines, a diferència de l'eina en aquest projecte que ha detectat 33 pàgines web. Amb aquesta prova es detecta que les extensions de detecció de minat actuals no són tan eficients, ja que utilitzen un mètode (*blacklist*) que és molt fàcil de sobrepassar.

A més més s'ha finalitzat el projecte analitzant l'impacte que té la pàgina més popular trobada. Els beneficis són molt baixos actualment comparat amb altres alternatives com pot ser la publicitat. A més a més el consum elèctric és bastant elevat.

21. Treball futur

Com a treball futur es podria utilitzar el projecte ampliant-lo per detectar altres amenaces que existeixen per internet com per exemple el *web tracking*.

També seria possible modifica l'extensió actual perquè informes de les pàgines minant i es podria incloure en els navegadors Chrome i Firefox per ser utilitzada per qualsevol persona.

22. Agraïments

M'agradaria expressar la meva gratitud al professor Pere-Barlet Ros i al professor Josep Solé Pareta per la orientació constant i crítiques útils aportades durant la realització del projecte que han estat essencials per obtenir uns resultats favorables.

També agraeixo la col·laboració oferta pel doctorand Ismael Castillo en el desenvolupament de l'eina.

Finalment, vull agrair especialment el suport per part de la família i amics que han estat al costat.

23. Bibliografia

- [1] "Alexa Top 500 Global Sites." [Online]. Available: <https://www.alexa.com/topsites>. [Accessed: 19-Feb-2019].
- [2] "Internet Security Threat Report ISTR Cryptojacking: A Modern Cash Cow An ISTR Special Report |," 2018.
- [3] "Browser-Based Cryptocurrency Mining Makes Unexpected Return from the Dead | Symantec Blogs." [Online]. Available: <https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency>. [Accessed: 20-Feb-2019].
- [4] "Opt-in cryptomining script Coinhive 'barely used' say researchers • The Register." [Online]. Available: https://www.theregister.co.uk/2018/02/27/ethical_coinhive/. [Accessed: 20-Feb-2019].
- [5] "Popular 'cryptojacking' service Coinhive will shut down next week - The Verge." [Online]. Available: <https://www.theverge.com/2019/2/28/18244636/coinhive-cryptojacking-cryptocurrency-mining-shut-down-monero-date>. [Accessed: 20-Jun-2019].
- [6] "Wappalyzer - Cryptominer." [Online]. Available: <https://www.wappalyzer.com/categories/cryptominer>. [Accessed: 22-Jun-2019].
- [7] "The State of Cryptojacking." [Online]. Available: <https://crypto.adguard.com/>. [Accessed: 21-Feb-2019].
- [8] X. Lou, J. Zhang, S. Liu, N. Xu, and D. J. Liao, "The other side of the coin: A framework for detecting and analyzing web-based cryptocurrency mining campaigns," *Int. Conf. Availability, Reliab. Secur.*, 2018.
- [9] "The WebSocket API (WebSockets) - Web APIs | MDN." [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API. [Accessed: 23-Feb-2019].
- [10] Y. Nan *et al.*, "How You Get Shot in the Back," *CCS '18 (ACM Conf. Comput. Commun. Secur.*, pp. 1701–1713, 2018.
- [11] "No Coin Alternatives and Similar Software - AlternativeTo.net." [Online]. Available: <https://alternativeto.net/software/no-coin/>. [Accessed: 23-Feb-2019].
- [12] "MinerBlock Alternatives and Similar Software - AlternativeTo.net." [Online]. Available: <https://alternativeto.net/software/minerblock/>. [Accessed: 23-Feb-2019].

- [13] "Selenium WebDriver." [Online]. Available: <https://www.seleniumhq.org/projects/webdriver/>. [Accessed: 02-Mar-2019].
- [14] "Copisteria online." [Online]. Available: <https://copytop.es/copisteria/copisteria-online-barata-1436>. [Accessed: 10-Mar-2019].
- [15] "Pricing Calculator | Microsoft Azure." [Online]. Available: <https://azure.microsoft.com/es-es/pricing/calculator/#virtual-machines1>. [Accessed: 10-Mar-2019].
- [16] A. E. Buxó, "Uncovering obfuscated web tracking," UPC, 2016.
- [17] "Home | Monero - secure, private, untraceable." [Online]. Available: <https://www.getmonero.org/>. [Accessed: 21-Jun-2019].
- [18] "CryptoNight - Bitcoin Wiki." [Online]. Available: <https://en.bitcoin.it/wiki/CryptoNight>. [Accessed: 21-Jun-2019].
- [19] "JSEcoin is a cryptocurrency mined by webmasters and built for everyone," 2017.
- [20] "Gunicorn - Python WSGI HTTP Server for UNIX." [Online]. Available: <https://gunicorn.org/>. [Accessed: 24-Jun-2019].
- [21] "Cross-Origin Resource Sharing (CORS) - HTTP | MDN." [Online]. Available: <https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS>. [Accessed: 24-Jun-2019].
- [22] "PhilGrayson/chrome-csp-disable: Disable Content-Security-Policy in Chromium browsers for web application testing." [Online]. Available: <https://github.com/PhilGrayson/chrome-csp-disable>. [Accessed: 24-Jun-2019].
- [23] "Notmining || Check if your website was infected." [Online]. Available: <https://notmining.es/>. [Accessed: 24-Jun-2019].
- [24] "Computer Power Consumption: How Much Energy Computers Consume." [Online]. Available: <https://www.kompulsa.com/much-power-computers-consume/>. [Accessed: 27-Jun-2019].
- [25] "Cinecalidad.to Analytics - Market Share Stats & Traffic Ranking." [Online]. Available: <https://www.similarweb.com/website/cinecalidad.to>. [Accessed: 27-Jun-2019].
- [26] "Consumo de electricidad medio de una vivienda en España." [Online]. Available: <https://tarifasgasluz.com/faq/consumo-electricidad-hogares/espana>. [Accessed: 27-Jun-2019].
- [27] "CryptoLoot - Earn More From Your Traffic." [Online]. Available: <https://cryptolootminer.com/>. [Accessed: 27-Jun-2019].

